

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-187826

(43) 公開日 平成10年(1998) 7月21日

(51) Int.Cl.<sup>8</sup>

識別記号

F I

G 0 6 F 17/60

19/00

G 0 6 K 17/00

G 0 7 D 9/00

G 0 7 F 7/12

4 6 1

G 0 6 F 15/21

G 0 6 K 17/00

G 0 7 D 9/00

G 0 6 F 15/30

G 0 7 F 7/08

3 4 0 C

S

4 6 1 Z

3 3 0

C

審査請求 有 請求項の数 5 F D (全 13 頁)

(21) 出願番号

特願平8-354467

(22) 出願日

平成 8 年(1996) 12月19日

(71) 出願人 000004237

日本電気株式会社

東京都港区芝五丁目 7 番 1 号

(72) 発明者 島田 道雄

東京都港区芝五丁目 7 番 1 号 日本電気株

式会社内

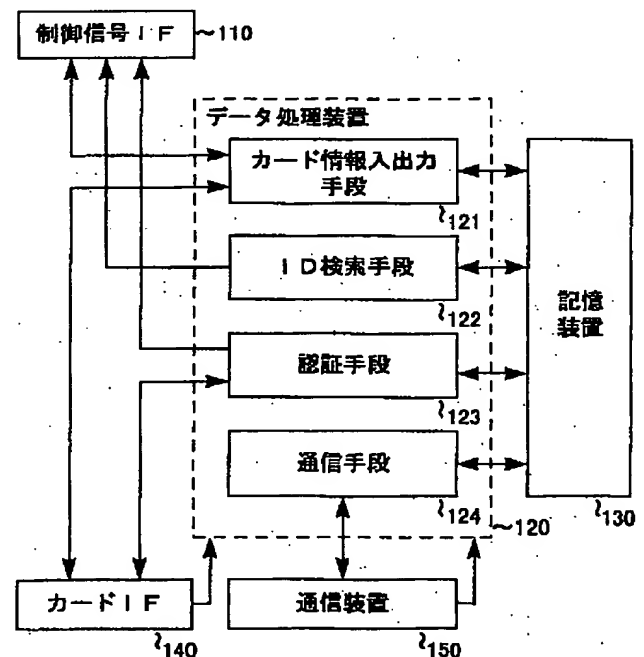
(74) 代理人 弁理士 境 廣巳

(54) 【発明の名称】 偽造カード使用防止方法およびカード読取書込装置ならびに偽造カード使用防止システム

(57) 【要約】

【課題】 センタ装置とリアルタイムで通信しないで、また、カード内部で高度な暗号化を行わないで、偽造カードの使用を困難にする。

【解決手段】 ICカードの使用時、カード読取書込装置のID検索手段122は、カードのIDが記憶装置130に記憶されているブラックリストに登録されているか否かを調べ、登録されていれば偽造カードであると判定する。また、認証手段123は、カードと通信を行ってカードを認証し、もし、カードが認証されなかったら、偽造カードであると判定する。通信手段124は、センタ装置と非リアルタイムで通信し、センタ装置にカード情報を送信するとともに、センタ装置からブラックリストに追加するIDを受信する。



**【特許請求の範囲】**

**【請求項 1】** カードの不正な使用を防止する方法において、

カード読取書込装置によってカードから取得したIDや使用履歴などのカード情報を非リアルタイムにセンタ装置に送信し、センタ装置においてカードの使用履歴の推移を評価して論理的な矛盾を含むカードのIDをブラックIDとして検出してカード読取書込装置に送信することで、カード読取書込装置の保持するブラックリストを逐次更新し、

カードの使用時は、カード読取書込装置において、そのカードのIDとブラックリスト中のIDとの比較によって不正なカードを検出すると共に、更に、カードとの通信によってそのカードが正規のものか否かを識別する認証を行うことを特徴とする偽造カード使用防止方法。

**【請求項 2】** カードの不正な使用を防止する機能を有するカード読取書込装置であって、

カードの使用者に対してサービスを提供する外部装置との通信を行うための制御信号インタフェースと、

カードとの通信を行うためのカードインタフェースと、センタ装置との通信を行うための通信装置と、

前記センタ装置から送られてきた偽造カードにかかるIDを登録してあるブラックリストを記憶する記憶装置と、

前記カードインタフェースを介してカードに記憶されているIDや使用履歴などのカード情報を読み取って前記記憶装置に記憶するとともに、予め決められた手順にもとづいてカード情報を書き換えて、書き換えられたカード情報を前記カードインタフェースを介してカードに書き込むカード情報入出力手段と、

カードのIDが前記記憶装置に記憶されているブラックリストに存在するか否かを検索して、もし、存在すれば、カードが偽造カードであることを示すための制御信号を前記制御信号インタフェースに送出するID検索手段と、

前記カードインタフェースを介してカードと通信を行ってカードを認証し、もし、カードが認証されなかったら、カードが偽造カードであることを示すための制御信号を前記制御信号インタフェースに送出する認証手段と、

前記通信装置を介してセンタと非リアルタイムで通信して、センタに前記記憶装置に記憶されたカード情報を送信するとともに、センタから前記ブラックリストに追加するIDを受信する通信手段とを備えることを特徴とするカード読取書込装置。

**【請求項 3】** カードの不正な使用を防止するシステムにおいて、

センタ装置と、カードの使用者に対してサービスを提供する外部装置および前記センタ装置に通信可能に接続された複数のカード読取書込装置とを含み、

前記カード読取書込装置は、

前記外部装置との通信を行うための制御信号インタフェースと、

カードとの通信を行うためのカードインタフェースと、記憶装置と、

前記センタ装置との通信を行うための通信装置と、

前記カードインタフェースを介してカードに記憶されているIDや使用履歴などのカード情報を読み取って前記記憶装置に記憶するとともに、予め決められた手順にもとづいてカード情報を書き換えて、書き換えられたカード情報を前記カードインタフェースを介してカードに書き込むカード情報入出力手段と、

カードのIDが前記記憶装置に記憶されているブラックリストに存在するか否かを検索して、もし、存在すれば、カードが偽造カードであることを示すための制御信号を前記制御信号インタフェースに送出するID検索手段と、

前記カードインタフェースを介してカードと通信を行ってカードを認証し、もし、カードが認証されなかったら、カードが偽造カードであることを示すための制御信号を前記制御信号インタフェースに送出する認証手段と、

前記通信装置を介してセンタと非リアルタイムで通信して、センタに前記記憶装置に記憶されたカード情報を送信するとともに、センタから前記ブラックリストに追加するIDを受信する通信手段とを備え、

前記センタ装置は、

前記カード読取書込装置との通信を行うための通信装置と、

記憶装置と、

該記憶装置に記憶されている新しく使われたカードの使用履歴をID順に並べ替える新履歴ソート手段と、

前記記憶装置に記憶されている過去に使われたカードの使用履歴に、前記新履歴ソート手段でソートされた、新しく使われたカードの使用履歴を追加する新履歴と旧履歴のマージ手段と、

使用履歴が追加されたカードについてカードの使用履歴の推移を評価して、論理的な矛盾が無いかな否かを検出し、もし矛盾が検出されたら、そのカードのIDを、前記記憶装置に記憶されているマスターブラックリストに登録する矛盾検出手段と、

前記通信装置を介して前記カード読取書込装置と非リアルタイムに通信して、前記カード読取書込装置からカード情報を受信して前記記憶装置に記憶するとともに、前記マスターブラックリストに新たに登録されたIDを前記カード読取書込装置に送信する通信手段とを備え、

前記カードは、

前記カード読取書込装置との間の通信を行うためのインタフェースと、

記憶装置と、

該記憶装置に記憶されているIDや使用履歴などのカード情報を前記インタフェースを介して前記カード読取書込装置に送信するカード情報送信手段と、  
新しいカード情報を前記インタフェースを介して前記カード読取書込装置から受信して前記記憶装置に書き込むカード情報受信手段と、  
前記インタフェースを介して前記カード読取書込装置と通信を行ってカードの認証を行う認証手段とを備えることを特徴とする偽造カード使用防止システム。

【請求項4】 前記カード読取書込装置の認証手段は、入力される暗号鍵Kにもとづいて、入力されるカードIDを暗号化して、暗号文を出力する暗号化手段と、乱数 $r$ を生成する乱数生成手段と、該生成された乱数 $r$ をカードに送信して、それに対するカードの出力 $x$ を受信する手段と、前記暗号化手段から出力された暗号文のうち前記生成された乱数 $r$ で指定される位置のビット列を選択して出力するセレクトと、該セレクトの出力とカードの前記出力 $x$ を比較する比較器とを備え、  
前記カードの認証手段は、予めデータの書き込まれたメモリを備え、前記カード読取書込装置の送信した乱数 $r$ を前記メモリのアドレスとして、それに対応する前記メモリのデータ出力 $x$ を前記カード読取書込装置に送信する構成を有することを特徴とする請求項3記載の偽造カード使用防止システム。

【請求項5】 カードとの通信を行うためのカードインタフェースと、該カードインタフェースを介して署名対象カードから読み込んだカードIDと別途入力された暗号鍵にもとづいて前記カードIDを暗号化する手段とを備え、暗号化によって得られた暗号文を前記カードインタフェースを介して署名対象カードの前記メモリに書き込む構成を有するカード署名装置を備えたことを特徴とする請求項4記載の偽造カード使用防止システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、料金の支払いや身分証明のために用いられるICカードを偽造して不正に使用することを防止する技術に関する。

【0002】

【従来の技術】 我々の身の回りでは、良く知られているように、磁気カードやICカードが、現金や身分証明書の代替として広く使用されている。これらのカードは、しばしば、店員などの人手を介さずに、公衆電話や自動改札機や現金支払機などに投入されて使われる。そのような使われ方がされる用途では、カードの精巧な複製を製造しなくても、カードのデータを別のカードに電子的に複製することで、偽造カードが簡単に製造できるため、偽造カードを製造して不正に利益を得ようとする不心得な者が後を断たない。

【0003】 そこで、クレジットカードでは、センタにカードのIDや有効期限や所有者名や使用履歴などのカード情報を登録・照会することが行われていた。なお、IDとは、それぞれのカードに予め割り当てられたカード固有の番号のことである。このようにすれば、偽造カードのIDが一旦センタに登録されれば、その偽造カードが使えなくなる。このようなカードの不正な使用を防止する方法としては、例えば特開平3-25568号公報に記載のものがあ

る。

【0004】 また、クレジットカードでは、カード会社しか知らない暗号鍵でIDなどのカード情報を暗号化して得られるデータをカードに記録することが行われていた。このようにすれば、カード会社以外の者が新しいIDを持つカードを不正に発行することができなくなる。このような防止方法としては、例えば特開平1-262886号公報や特開昭62-188070号公報に記載のものがあ

る。

【0005】 なお、カードの偽造には、正規のカードと同じものを複製するものや、正規のカードのデータを書き換えてカードの価値を大きくするものや（狭義には変造と呼ぶ）、新しいIDを持つカードを製造するものがあるが（狭義には偽造と呼ぶ）、以下では特に断りの無い限り、すべてを偽造と呼ぶことにする。

【0006】 また、認証とは、カードと通信することによって、そのカードが正規のものか否かを識別する技術である。暗号とは、暗号鍵に依存して、データ（平文と呼ぶ）を別のデータ（暗号文と呼ぶ）に変換するもので、暗号文から平文が容易に推定できず、また、平文と暗号文から暗号鍵が容易に推定できないような変換のことである。なお、認証や暗号については、例えば、昭見堂から1990年に発行された辻井、笠原編著「暗号と情報セキュリティ」などに詳しい解説がある。

【0007】

【発明が解決しようとする課題】 センタを設置して、カードの使用履歴を問い合わせることで、偽造カードの使用を検出する方法は、クレジットカードならともかく、小額の支払いに用いられるカードシステムには、通信コスト上の問題があるので適用できないという問題があったし、交通料金の支払いに用いられるカードシステムのように短時間で処理しなければならないカードシステムには、センタとの通信に時間がかかるために、適用できないという問題があった。

【0008】 また、カードのIDを暗号化して記録する従来の方法では、偽造者がIDを自由に選択することは防げるものの、カードを複製して偽造カードを製造することは防げないため、そのような不正な使用を防止することはできなかった。

【0009】 また、認証によってのみカードの不正な使用を防止する方法は、防止効果を高めるために、暗号化のための複雑な処理や多桁整数の四則演算を必要とする

ので、IDカードに搭載されている8ビットのマイクロコンピュータで高速処理することは困難であるという問題があった。

【0010】本発明は、以上の問題点を解決し、運用コストが小さくて高速に処理できる偽造カード使用防止技術を提供することを目的とする。

【0011】

【課題を解決するための手段】本発明は、偽造カードの使用を防止する方法において、カード読取書込装置(図13の1)によってカード(図13の2)から取得したIDや使用履歴などのカード情報を非リアルタイムにセンタ装置(図13の3)に送信し、センタ装置においてカードの使用履歴の推移を評価して論理的な矛盾を含むカードのIDをブラックIDとして検出してカード読取書込装置に送信することで、カード読取書込装置の保持するブラックリストを逐次更新し、カードの使用時は、カード読取書込装置において、そのカードのIDとブラックリスト中のIDとの比較によって不正なカードを検出すると共に、更に、カードとの通信によってそのカードが正規のものか否かを識別する認証を行うことを特徴とする。

【0012】また、カードの不正な使用を防止する機能を有する本発明のカード読取書込装置は、カードの使用に対してサービスを提供する外部装置(図13の4)との通信を行うための制御信号インタフェース(図1の110)と、カードとの通信を行うためのカードインタフェース(図1の140)と、センタ装置との通信を行うための通信装置(図1の150)と、前記センタ装置から送られてきた偽造カードにかかるIDを登録してあるブラックリストを記憶する記憶装置(図1の130)と、前記カードインタフェースを介してカードに記憶されているIDや使用履歴などのカード情報を読み取って前記記憶装置に記憶するとともに、予め決められた手順にもとづいてカード情報を書き換えて、書き換えられたカード情報を前記カードインタフェースを介してカードに書き込むカード情報入出力手段(図1の121)と、カードのIDが前記記憶装置に記憶されているブラックリストに存在するか否かを検索して、もし、存在すれば、カードが偽造カードであることを示すための制御信号を前記制御信号インタフェースに送出するID検索手段(図1の122)と、前記カードインタフェースを介してカードと通信を行ってカードを認証し、もし、カードが認証されなかったら、カードが偽造カードであることを示すための制御信号を前記制御信号インタフェースに送出する認証手段(図1の123)と、前記通信装置を介してセンタと非リアルタイムで通信して、センタに前記記憶装置に記憶されたカード情報を送信するとともに、センタから前記ブラックリストに追加するIDを受信する通信手段(図1の124)とを備えることを特徴とする。

【0013】また、本発明は、偽造カードの使用を防止するシステムにおいて、センタ装置(図13の3)と、カード(図13の2)の使用に対してサービスを提供する外部装置(図13の4)および前記センタ装置に通信可能に接続された複数のカード読取書込装置(図13の1)とを含み、前記カード読取書込装置は、前記外部装置との通信を行うための制御信号インタフェース(図1の110)と、カードとの通信を行うためのカードインタフェース(図1の140)と、記憶装置(図1の130)と、前記センタ装置との通信を行うための通信装置(図1の150)と、前記カードインタフェースを介してカードに記憶されているIDや使用履歴などのカード情報を読み取って前記記憶装置に記憶するとともに、予め決められた手順にもとづいてカード情報を書き換えて、書き換えられたカード情報を前記カードインタフェースを介してカードに書き込むカード情報入出力手段(図1の121)と、カードのIDが前記記憶装置に記憶されているブラックリストに存在するか否かを検索して、もし、存在すれば、カードが偽造カードであることを示すための制御信号を前記制御信号インタフェースに送出するID検索手段(図1の122)と、前記カードインタフェースを介してカードと通信を行ってカードを認証し、もし、カードが認証されなかったら、カードが偽造カードであることを示すための制御信号を前記制御信号インタフェースに送出する認証手段(図1の123)と、前記通信装置を介してセンタと非リアルタイムで通信して、センタに前記記憶装置に記憶されたカード情報を送信するとともに、センタから前記ブラックリストに追加するIDを受信する通信手段(図1の124)とを備え、前記センタ装置は、前記カード読取書込装置との通信を行うための通信装置(図6の650)と、記憶装置(図6の630)と、該記憶装置に記憶されている新しく使われたカードの使用履歴をID順に並べ替える新履歴ソート手段(図6の621)と、前記記憶装置に記憶されている過去に使われたカードの使用履歴に、前記新履歴ソート手段でソートされた、新しく使われたカードの使用履歴を追加する新履歴と旧履歴のマージ手段(図6の622)と、使用履歴が追加されたカードについてカードの使用履歴の推移を評価して、論理的な矛盾が無いかな否かを検出し、もし矛盾が検出されたら、そのカードのIDを、前記記憶装置に記憶されているマスターブラックリストに登録する矛盾検出手段(図6の623)と、前記通信装置を介して前記カード読取書込装置と非リアルタイムに通信して、前記カード読取書込装置からカード情報を受信して前記記憶装置に記憶するとともに、前記マスターブラックリストに新たに登録されたIDを前記カード読取書込装置に送信する通信手段(図6の624)とを備え、前記カードは、前記カード読取書込装置との間の通信を行うためのインタフェース(図4の410)と、記憶装置(図4の430)と、該

記憶装置に記憶されているIDや使用履歴などのカード情報を前記インタフェースを介して前記カード読取書込装置に送信するカード情報送信手段(図4の421)

と、新しいカード情報を前記インタフェースを介して前記カード読取書込装置から受信して前記記憶装置に書き込むカード情報受信手段(図4の422)と、前記インタフェースを介して前記カード読取書込装置と通信を行ってカードの認証を行う認証手段(図4の423)とを備えることを特徴とする。

【0014】また、前記カード読取書込装置の認証手段は、入力される暗号鍵Kにもとづいて、入力されるカードIDを暗号化して、暗号文を出力する暗号化手段(図11の1102)と、乱数rを生成する乱数生成手段(図11の1101)と、該生成された乱数rをカードに送信して、それに対するカードの出力xを受信する手段(図11の1107、1108)と、前記暗号化手段から出力された暗号文のうち前記生成された乱数rで指定される位置のビット列を選択して出力するセレクト

(図11の1103)と、該セレクトの出力とカードの前記出力xを比較する比較器(図11の1104)とを備え、前記カードの認証手段は、予めデータの書き込まれたメモリ(図10の1002)を備え、前記カード読取書込装置の送信した乱数rを前記メモリのアドレスとして、それに対応する前記メモリのデータ出力xを前記カード読取書込装置に送信する構成を有することを特徴とする。

【0015】さらに、カードとの通信を行うためのカードインタフェース(図12の1202)と、該カードインタフェースを介して署名対象カードから読み込んだカードIDと別途入力された暗号鍵にもとづいて前記カードIDを暗号化する手段(図12の1201)とを備え、暗号化によって得られた暗号文を前記カードインタフェースを介して署名対象カードの前記メモリに書き込む構成を有するカード署名装置を備えている。

【0016】

【作用】従来の偽造カード使用防止技術は、偽造カードの使用が確実に検出できることを目指して設計されていた。しかしながら、偽造カードの使用を確実に検出しようとするからこそ、その不正使用を防止するためのコストが大きくなったり、不正使用の検出に要する時間が長くなると考えられる。そこで、本発明では、発想を転換して、偽造カードの使用を大きな確率で検出できればよしとする。もちろん、クレジット・カードのように、1回あたりの取引額が大きいシステムの場合には、偽造カードの利用者が高額な商品を大量に購入して行方をくらます可能性もあるので、偽造カードの使用を確実に検出しなければならないが、1回あたりの取引額が小さいシステム(市内バスや地下鉄などのプリペイドカードシステム等)の場合には、偽造カードの使用を確実に検出する必要はないのである。なぜなら、1回あたりの取引額

が小さい場合には、偽造カードの利用者は、一般に、不正に得られる利益を大きくするために頻りに偽造カードを使用するので、1回の使用につき或る程度の確率で偽造カードの使用が検出できれば、いつかは偽造カードの使用が検出できるからである。しかも、偽造カードの利用者を拘束できるシステム(例えばカードで交通機関の運賃を支払うようなシステム)においては、偽造カードの利用者から罰金を徴収することによって、偽造カードの使用による過去の損失も補填できるからである。もちろん、偽造カードの使用を確実に検出できないと、少数の利用者が偽造カードを稀に使用している場合には、偽造カードの使用を高い確率で見逃してしまうかもしれない。例えば、悪意を持つ正規の利用者が、プリペイドカードの残高がほとんどゼロになった時に、カードに記録されている残高の額を大きくすれば、そのカードは1回あるいは何回か不正使用されてしまうかもしれない。しかしながら、そのような場合には、偽造カードの使用による損失が極めて小さいので、たとえ検出できなくてもカード・システムの運営者の利益はほとんど損なわれない。なお、偽造カードの使用という不正行為を確率的に見逃してしまうことは、心理的には許容しがたいことかもしれないが、カード・システムの運営者の利益を考慮すると、「不正使用防止のためのコスト」を度外視して「偽造カードの使用による損失」だけを小さくするのはなく、「不正使用防止のためのコスト」と「偽造カードの使用による損失」との合計を小さくすべきなのである。従って、本発明によって「不正使用防止のためのコスト」が大幅に削減できるのであれば、経済的には、そのような見逃しは許容されるであろう。

【0017】そこで、本発明では、まず、センタを用いる不正使用防止システムにおいて、偽造カードの判定基準を緩くする。すなわち、本発明におけるカード読取書込装置は、カードが入力されるごとにセンタ装置と通信するのではなく、入力されたカードのIDがカード読取書込装置の記憶装置に記憶されているブラックリストに登録されているか否かを調べ、もし、ブラックリストにIDが存在すれば偽造カードと判定する。また、カード読取書込装置は、カードのIDや使用履歴などのカード情報をセンタ装置に送信する。センタ装置への送信は、カード読取書込装置にカードが入力されることに行っても良いし、一定時間ごとに行っても良いし、カード情報が一定量だけ蓄積されてから行っても良いし、センタ装置がカード読取書込装置と通信する際に行っても良い。また、通信コストが大きい場合には、カード読取書込装置からセンタ装置へ、すべてのカードのIDや使用履歴などのカード情報を送信しないで、一部のカードのIDや使用履歴だけを送信しても良い。そして、センタ装置は、カード読取書込装置から送信されるカードのIDや使用履歴などのカード情報にもとづいて、偽造カードが使用されたかどうかを判定し、もし偽造カードが存在す

れば、その偽造カードのIDを、センタ装置側のマスターブラックリストに登録する。また、センタ装置は、カード読取書込装置と定期的に通信して、前回の通信から現時点までにマスターブラックリストに加わった新しいIDをカード読取書込装置に送ってそのブラックリストに登録する。このようにすれば、カード読取書込装置とセンタ装置とがリアルタイムで通信する必要がなくなるので、通信コストも節約できるし、不正使用の判定に要する時間も短く済む。もちろん、以上のようにすると、偽造カードのIDがカード読取書込装置側のブラックリストに登録されるまで、その偽造カードの使用を見逃してしまうのだが、カードを1回使用することに取り引きされる金額が小さく、ブラックリストの更新時間の間隔が長くなければ、偽造カードによる損害を無視できるほど小さく抑えられる。

【0018】もっとも、以上のような「センタを用いた不正使用防止方法」は、十分な防止効果を持っていないし、偽造カードが大量に使われると経済的な損失を受けるだけでなくカードシステムを正常に運営すること自体が困難になる。というのも、本発明においては、カード読取書込装置のブラックリストは瞬時に更新されないで、カードの偽造者が、正規のカードとカード読取書込装置の間の通信を盗聴し、盗聴によって得られたカード情報にもとづいて偽造カードを作成して、その偽造カードを使うことが考えられるからである。非接触型のICカードを用いたカードシステムでは、盗聴による偽造は容易である。もちろん、その偽造カードは、ブラックリストが更新されるまでしか、正規のカードとして通用しない。しかしながら、それ故に、カードの偽造者は、多くのIDを取得して多数の偽造カードを製造することになる。そして、それらの偽造カードが使われて、それらのIDがカード読取書込装置のブラックリストに登録されてしまうと、多数の正規のカードが使えなくなってしまう。カードの偽造者によって悪用されたIDが非常に多いと、正規のカードを偽造カードであると判定することが頻繁に発生して、カードシステムの機能が麻痺することも考えられる。以上のような「センタを用いた不正使用防止方法」がこれまで使われなかったのも、おそらく、そのような問題があったからであろう。

【0019】そこで、本発明では、以上で述べた「センタを用いた不正使用防止方法」に加えて、「認証を用いた不正使用防止方法」を併用することで、偽造カードの使用を検出することにする。認証を併用することは、一見すると、経済性と不正使用防止効果を両立できないように思われる。なぜなら、第1に、現在の認証技術をもってすれば、認証だけでもカードの不正使用を極めて困難にできるので、不正使用防止効果の高い認証方法を用いるのであれば、わざわざセンタを設置する必要なぞないからである。第2に、装置化の容易な簡便な認証方法を採用すれば経済性は損なわれないものの、そのような

認証方法には不正使用防止の効果がほとんど無いように思われるからである。しかしながら、本発明においては、カード読取書込装置のブラックリストが更新されるまでの短い期間における偽造カードの使用が、認証によって検出できれば良いのであるし、既に述べたような理由から、偽造カードの使用が大きな確率で検出できれば十分なのであるから、簡便な認証方法を利用できる。

#### 【0020】

【発明の実施の形態】次に、本発明の実施例について図面を参照して詳細に説明する。

【0021】図13は、本発明の偽造カード使用防止システムの一例を示す全体構成図である。この例の偽造カード使用防止システムは、複数のカード読取書込装置1と、これら複数のカード読取書込装置1と有線または無線によって通信可能なセンタ装置3とから構成されている。なお、2はカードを、4はカード2の使用者に対してサービスを提供する外部装置（例えば自動販売機や改札機など）をそれぞれ示す。

【0022】本例の偽造カード使用防止システムにおいては、各カード読取書込装置1によってカード2から取得したIDや使用履歴などのカード情報を非リアルタイムにセンタ装置3に送信し、センタ装置3においてカードの使用履歴の推移を評価して論理的な矛盾を含むカードのIDをブラックIDとして検出して各カード読取書込装置1に送信することで、各カード読取書込装置1の保持するブラックリストを逐次更新する。なお、カード情報中の使用履歴には、カード使用日時、使用場所を定める情報（例えば各カード読取書込装置に振られた番号など）、利用金額などが含まれる。そして、カード2の使用時は、各カード読取書込装置1において、そのカードのIDとブラックリスト中のIDとの比較によって不正なカードを検出すると共に、更に、カード2との通信によってそのカードが正規のものか否かを識別する認証を行う。偽造カードと判定された場合には外部装置4に制御信号が出され、当該カードを受け付けないようにする処理や警報を発する処理などが外部装置4において行われることにより、偽造カードによる不正な使用を防止する。

【0023】以下、カード読取書込装置1、カード2およびセンタ装置3の構成例について詳述する。

【0024】図1は、カード読取書込装置の実施例の基本構成を示す機能ブロック図である。この実施例のカード読取書込装置は、制御信号インタフェース（以下では略して制御信号IFと呼ぶ）110と、データ処理装置120と、記憶装置130と、カードインタフェース（以下では略してカードIFと呼ぶ）140と、通信装置150とから構成されている。

【0025】制御信号IF110は、自動販売機や改札機などカードの使用者に対してサービスを提供する外部装置とデータ処理装置120との間の通信を行うための

回路である。カードIF140は、カードとデータ処理装置120との間の通信を行うための回路である。記憶装置130は、ランダム・アクセス・メモリとリード・オンリ・メモリ（以下ではROMと呼ぶ）によって構成され、データ処理装置120の出力するデータを記憶したり、記憶したデータをデータ処理装置120に供給する。通信装置150は、センタとデータ処理装置120との間の通信を行うための装置である。

【0026】データ処理装置120は、マイクロプロセッサによって構成され、予めROMに書かれた命令に従って、本カード読取書込装置全体の制御を行う。すなわち、データ処理装置120には、カードIF140を介してカードに記憶されているIDや使用履歴などの情報を読み取って記憶装置130に記憶するとともに、必要ならば、自動販売機や改札機などカードの利用者に対してサービスを提供する装置から制御信号IF110を介して供給される料金および現在日時などの情報に基づいて、カード情報の使用履歴などを書き換えて、書き換えられたデータをカードIF140を介してカードに書き込むカード情報入出力手段121と、カードのIDが記憶装置130に記憶されているブラックリストに存在するか否かを検索して、もし、存在すれば、カードが偽造カードであることを示すための制御信号を制御信号IF110に送出するID検索手段122と、カードIF140を介してカードと通信を行ってカードを認証し、もし、カードが認証されなかったら、カードが偽造カードであることを示すための制御信号を制御信号IF110に送出する認証手段123と、通信装置150を介してセンタと通信して、センタに対し記憶装置130に記憶されたカード情報を送信するとともに、センタからブラックリストに追加するIDを受信してブラックリストに追加する通信手段124とが、予めROMに書かれた命令によって、実現されている。

【0027】図2は、図1のカード読取書込装置の動作のうち偽造カードの検出に関する動作を説明するフローチャートである。図において、カードIF140がカードが入力されたことを示す制御信号をデータ処理装置120に供給したら、データ処理装置120は、まず、カード情報入出力手段121によって、カードIF140を介してカードに記憶されているIDや使用履歴などの情報を読み取って記憶装置130に記憶するとともに、必要ならば、自動販売機や改札機などカードの利用者に対してサービスを提供する操作から制御信号IF110を介して供給される料金などの情報にもとづいて、カード情報を書き換えて、書き換えられたデータをカードIF140を介してカードに書き込む（201）。次に、ID検索手段122によって、当該カードのIDが記憶装置130に記憶されているブラックリストに存在するか否かを検索して（202）、もし、存在すれば、制御を手順206に移し、さもなくば、制御を手順204に

移す（203）。

【0028】手順204では、データ処理装置120は、認証手段123によって、カードIF140を介してカードと通信を行ってカードを認証する。そして、もし、カードが認証されなかったら、制御を手順206に移し、さもなくば、処理を終了する（205）。他方、手順206においては、データ処理装置120は、カードが偽造カードであることを示すための制御信号を制御信号IF110に送出して、処理を終了する。

【0029】図3は、図1のカード読取書込装置の動作のうちセンタとの通信に関する動作を説明するフローチャートである。図において、通信装置150がセンタからの通信が入ったことを示す制御信号をデータ処理装置120に供給したら、データ処理装置120は、通信手段124によって、通信装置150を介してセンタと通信して、記憶装置130に記憶されていたカード情報をセンタに送信して（301）、記憶装置130に記憶されていた上記カード情報を消去する（302）。次に、センタからブラックリストに追加するIDを受信し（303）、この受信したIDを記憶装置130に記憶されているブラックリストに登録して（304）、処理を終了する。

【0030】図4は、カードの実施例の基本構成を示す機能ブロック図である。この実施例のカードは、インタフェース（以下では略してIFと呼ぶ）410と、データ処理装置420と、記憶装置430とから構成されている。

【0031】IF410は、当該カードとカード読取書込装置との間の通信を行うための回路である。記憶装置430は、ランダム・アクセス・メモリとROMによって構成され、データ処理装置420の出力するデータを記憶したり、記憶したデータをデータ処理装置420に供給する。

【0032】データ処理装置420は、マイクロプロセッサによって構成され、予めROMに書かれた命令に従って、当該カードの制御を行う。すなわち、データ処理装置420には、記憶装置430に記憶されているIDや使用履歴などの情報をIF410を介してカード読取書込装置に送信するカード情報送信手段421と、新しいカード情報をIF410を介してカード読取書込装置から受信して記憶装置430に書き込むカード情報受信手段422と、IF410を介してカード読取書込装置と通信を行ってカードの認証を行う認証手段423とが、予めROMに書かれた命令によって、実現されている。なお、認証については後で詳しく述べるが、本実施例における認証手段423は、複雑な処理を必要としないので、データ処理装置420を、処理能力の低い8ビットのマイクロプロセッサで実現できる。

【0033】図5は、図4のカードの動作を説明するフローチャートである。図において、IF410を介して



カード読取書込装置から通信を要求する制御信号がデータ処理装置420に供給されたら、データ処理装置420は、カード情報送信手段421によって、記憶装置430に記憶されているIDや使用履歴などの情報をIF410を介してカード読取書込装置に送信し(501)、次に、カード情報受信手段422によって、新しいカード情報をIF410を介してカード読取書込装置から受信して記憶装置430に書き込む(502)。次に、認証手段423によって、IF410を介してカード読取書込装置と通信を行ってカードの認証を行い(503)、処理を終了する。なお、認証方法については後で詳しく述べるが、手順503における認証は、カード読取書込装置における図2の手順204における認証と対応するもので、同じ手順ではない。

【0034】図6は、センタ装置の実施例の基本構成を示す機能ブロック図である。この実施例のセンタ装置は、データ処理装置620と、記憶装置630と、通信装置650とから構成されている。

【0035】記憶装置630は、ランダム・アクセス・メモリやROMによって構成され、データ処理装置620の出力するデータを記憶したり、記憶したデータをデータ処理装置620に供給する。通信装置650は、データ処理装置620とカード読取書込装置との間の通信を行うための装置である。

【0036】データ処理装置620は、マイクロプロセッサによって構成され、予めROMに書かれた命令に従って、当該センタ装置の制御を行う。すなわち、データ処理装置620には、記憶装置630に記憶されている新しく使われたカードの使用履歴をID順に並べかえる新履歴ソート手段621と、記憶装置630に記憶されている過去に使われたカードの使用履歴に、新しく使われたカードの使用履歴を追加する、新履歴と旧履歴のマージ手段622と、使用履歴が追加されたカードについてカードの使用履歴の推移を評価して、論理的な矛盾が無いかなかを検出し、もし矛盾が検出されたら、そのカードのIDを、記憶装置630に記憶されているマスターブラックリストに登録する矛盾検出手段623と、通信装置650を介してカード読取書込装置と通信して、カード読取書込装置からカード情報を受信して記憶装置630に記憶するとともに、マスターブラックリストに新たに登録されたID(ブラックID)をカード読取書込装置に送信する通信手段624とが、予めROMに書かれた命令によって、実現されている。

【0037】図7は、図6のセンタ装置の動作のうち偽造カードの検出に関する動作を説明するフローチャートである。図において、データ処理装置620は、まず、新履歴ソート手段621によって、記憶装置630に記憶されている新しく使われたカードの使用履歴をID順に並べかえる(701)。次に、新履歴と旧履歴のマージ手段622によって、記憶装置630に記憶されてい

る過去に使われたカードの使用履歴に、新しく使われたカードの使用履歴を追加する(702)。次に、矛盾検出手段623によって、使用履歴が追加されたカードで手順703の処理がまだ行われていないカードについて、使用履歴の推移を評価して、論理的な矛盾が無いかなかを検出し(703)、もし矛盾が検出されたら、制御を手順705に移し、さもなければ制御を手順706に移す(704)。論理的な矛盾としては、例えば、同じIDのカードがほぼ同時刻に別々の場所(別々のカード読取書込装置)で使用されているといったことがあげられる。

【0038】次に、手順705では、矛盾の検出されたカードのIDを、記憶装置630に記憶されているマスターブラックリストに登録し(705)、制御を手順706に移す。手順706では、使用履歴が追加されたすべてのカードについて手順703が実行されたか否かを調べ、もし、使用履歴が追加されたすべてのカードについて手順703が実行済みであれば、処理を終了し、さもなければ、制御を703に移す。

【0039】図8は、図6のセンタ装置の動作のうちカード読取書込装置との間の通信に関する動作を説明するフローチャートである。図において、データ処理装置620は、まず、通信手段624によって、通信装置650を介して、カード読取書込装置との通信を開始し(801)、次に、カード読取書込装置から新しく使われたカードのカード情報を受信し(802)、次に、マスターブラックリストに新たに登録されたブラックIDをカード読取書込装置に送信し(803)、すべてのカード読取書込装置との通信が実行されたか否かを調べ、もし、すべてのカード読取書込装置との通信が実行済みであれば、処理を終了し、さもなければ、新しいカード読取書込装置を選択して、制御を801に移す(804)。

【0040】次に、カード読取書込装置とカードとの間において行われる認証について説明する。

【0041】図9は、図1のカード読取書込装置の認証手段123および図4のカードの認証手段423において用いられている認証方法を説明するシーケンスチャートである。図において、まず、カード読取書込装置が乱数 $r$ を生成して(901)、乱数 $r$ をカード $i$ に送信する(902)。なお、ここで、 $i$ はこのカードのIDとする。そして、カード $i$ は、カード読取書込装置から乱数 $r$ を受信し(902)、乱数 $r$ を関数 $S_i$ に入力して得られる出力 $x$ を求め(903)、 $x$ をカード読取書込装置に送信する(904)。カード読取書込装置は、 $x$ を受信して(904)、乱数 $r$ を関数 $S_i$ に入力して得られる出力と $x$ とを比較し(905)、もし、等しければ、通信相手のカードは正規のカードであると判定し、さもなければ、通信相手のカードは偽造カードであると判定する。なお、関数 $S_i$ はカード $i$ に固有な関数で、カード $i$ は、関数 $S_i$ だけを持っており、カード読取書込



装置は、すべての $i$ について、カード $i$ の関数 $S_i$ を持っている。

【0042】図10は、図4のカードの認証手段423の構成例を示す機能ブロック図である。本発明においては、カードが1回使用されるごとに確実にではなく或程度の確率で偽造カードが検出できれば良いから、関数 $S_i$ の入出力ビット数を小さくできる。図の実施例では、関数 $S_i$ は、カード読取書込装置から送信された8ビットの乱数 $r$ を入力端子1001を介して関数 $S_i$ 1002に入力して、出力端子1003に出力される8ビットの出力 $x$ をカード読取書込装置に送信している。なお、関数 $S_i$ の入出力ビット数が僅か8ビットなので、関数 $S_i$ 1002は、僅か256バイトの(1バイトは8ビットとする)ROM(1回書き込み可能なROM)で構築できる。つまり、ROM中に256バイトの関数 $S_i$ を保持し、8ビットの乱数 $r$ をアドレスとして、それに対応するROMの8ビットの出力を $x$ とする。

【0043】図11は、図1のカード読取書込装置における認証手段123の構成例を示す機能ブロック図である。図において、暗号関数1102は、入力端子1106から供給される暗号鍵 $K$ にもとづいて、入力端子1105から入力されるカードID(以下では $i$ とする)に対して暗号化を施して、得られた長さ256バイトの暗号文(後述するように正規のカードの場合は、この暗号文がカード署名装置によってカード $i$ の上記ROMに書き込まれている)を、セクタ1103に供給する。乱数発生器1101は、8ビットの乱数 $r$ を発生して、乱数 $r$ を出力端子1107を介してカードに送信するとともに、セクタ1103にも供給する。セクタ1103は、乱数 $r$ に依存して、暗号関数1102の出力する256バイトのうち1バイトを選択して、選択されたバイトを比較器1104に供給する。比較器1104のもう一方の入力には、カードから送信された $x$ が入力端子1108を介して供給されている。そして、比較器1104は、セクタ1103の出力と $x$ とを比較して、比較結果を出力端子1109から出力する。比較器1104が一致を検出した場合、当該カードは正規のカードであると判定される。以上のようにして、カード読取書込装置における認証手段123を実現すれば、カード読取書込装置にすべてのカードのROMの内容(関数 $S_i$ の内容)を記憶する必要が無い。

【0044】図12は、カードのROMに関数 $S_i$ (図10の1002)を書き込むためのカード署名装置の実施例を示す機能ブロック図である。図において、予めカードIDの書き込まれているカードが、カードインタフェース(以下ではカードIFと呼ぶ)1202に差し込まれると、カードIF1202を介して、カードIDが読み込まれて、読み込まれたカードIDが暗号関数1201に供給される。暗号関数1201は、図11の暗号関数1102と等価な暗号装置で、入力端子1203から

供給される暗号鍵 $K$ (図11の入力端子1106に加わる暗号鍵 $K$ と等価)にもとづいて、カードIDに暗号化を施して、得られた256バイトの暗号文を、カードIF1202を介して、カードの関数 $S_i$ (図10の1002)を構成しているROMに書き込まれる。

【0045】なお、以上の実施例においては、カードの関数 $S_i$ (図10の1002)を構成しているROMとして、1回書き込み可能なROMを用いたが、書き込んだ内容を保存できるものであれば、どのようなメモリを用いてもよい。また、以上の実施例においては、暗号関数の構成方法については述べなかったが、暗号関数の構成方法は、本発明と直接関係ないので、任意の暗号関数が使え。秘密鍵暗号を用いても良いし、必要ならば、公開鍵暗号を用いても良いし、フィードバック・シフトレジスタを用いても良い。なお、暗号関数をフィードバック・シフトレジスタで構成する場合には、例えば、フィードバック・シフトレジスタの係数を暗号鍵として、フィードバック・シフトレジスタの初期状態をカードIDとし、暗号文をフィードバック・シフトレジスタの出力とすれば良い。また、以上の実施例においては、暗号関数に供給する暗号鍵 $K$ を固定として考えていたが、暗号鍵 $K$ を定期的に変更しても良い。

【0046】また、以上の実施例においては、使用されたすべてのカードのカード情報をセンタ装置に送信していたが、偽造される危険性が少ない用途においては、選択された一部のカードのカード情報だけを送信することにより、センタ装置に送信する情報を削減することも可能である。例えば、カードIDのハッシュ値が予め定められた値をとるものについてだけ、カード情報を送信するのである。これは、すなわち、カード全体を検査するのではなく、一部のカードだけを抜き打ち検査することである。一人の偽造者が、多数のIDを利用して、偽造カードを製造している場合には、この方法でも、偽造カードを効果的に検出できる。

#### 【0047】

【発明の効果】第1の効果は、通信コストが小さく済むということである。なぜなら、センタを用いる従来の不正使用防止システムにおいては、端末からセンタに、すべてのカードのIDと使用履歴をリアルタイムで送信し、そのカードが正規のものかどうかの判定結果をセンタから受信しなければならなかったが、本発明においては、センタ装置のマスターブラックリストの移しを各カード読取書込装置が保持しており、ブラックリストによる偽造カードの検出に際して、センタ装置とリアルタイムで送信する必要がないからである。また、必要に応じて、一部のカードのIDと使用履歴だけを送信することで、送信するデータの量を削減できるからである。

【0048】第2の効果は、装置コストが小さくて済むということである。なぜなら、本発明は、ブラックリストによる偽造カードの検出を補完するためにカードの認

証を導入しており、認証手段は簡便なもので済むため、カードとカード読取書込装置との通信や認証において、複雑な暗号方式を使う必要が無いからである。もっとも、本発明は、カードの認証を行わなければならないので、磁気カードには適用できない。すなわち、本発明は、ICカードを用いたカードシステムにしか適用できない。しかしながら、本発明は、他のカードシステムと違い、認証暗号回路の搭載されている専用の高価なICカードを使わなくとも、8ビットのマイクロプロセッサしか搭載されていない汎用の安価なICカードでも、高い不正使用防止効果が発揮できるので、ICカードのコストが低下している今日においては、コストの問題はほとんど無視できる。特に、非接触型のICカードを使用した交通料金を支払うようなシステムにおいては、多くの場合、マイクロプロセッサや通信のための回路が搭載されているので、コストの問題はほとんど無視できる。

【0049】第3の効果は、高速に処理できるということである。なぜなら、既に述べたように、処理時間のかかる複雑な暗号方式を使う必要もないし、センタ装置とリアルタイムで通信する必要も無いからである。

【0050】第4の効果は、偽造カードの検出能力が高いということである。なぜなら、本発明のカード不正使用防止技術を無効にして、偽造カードを使用する方法は、以下で述べるように、原理的にはいくつか考えられるが、いずれの方法も、実際に実行することは難しいからである。第1の攻撃方法としては、偽造カードの使用者が、予め複数のカードの複製を作成しておき、それらを時間に応じて使い分けることが考えられる。もし、偽造カードの使用者のすべてが決められた時間に決められた偽造カードを使用し、一旦使用した偽造カードを2度と使わないようにすれば、カードの運営者が偽造カードの使用を検出してそのカードのIDをブラックリストに加えても、偽造カードの使用は防止できない。しかしながら、偽造カードの製造者は正規のカードを大量に調達しなければならないので、偽造カードの製造者が利益を得ることは難しい。また、仮に、偽造カードを大量生産して販売したとしても、カードの販売が発覚する危険が高くなるし、使用者の不注意や偽造カードを使用する時間のミスなどで、決められた時間に決められた偽造カードが使われないことが高い確率で生じ、多くの偽造カードの多くが使えなくなる。従って、ブラックリストが更新される時間の間隔が適切であれば、この攻撃方法は有効ではない。第2の攻撃方法は、大量の偽造カードを使用して、マスターブラックリストやブラックリストをオーバーフローさせて、偽造カード使用防止方法の運用を妨害する方法である。しかしながら、今日では大容量の記憶装置が安価に入手できるし、マスターブラックリストやブラックリストはIDだけのリストであるから、偽造カードの数を上回る膨大な数のIDを容易に記憶でき

る。従って、カード読取書込装置およびセンタ装置の記憶装置の記憶容量が適切に選択されていれば、そのような攻撃を実行するのは困難である。

#### 【図面の簡単な説明】

【図1】カード読取書込装置の実施例の基本構成を示す機能ブロック図である。

【図2】カード読取書込装置の動作のうち偽造カードの検出に関する動作を説明するフローチャートである。

【図3】カード読取書込装置の動作のうちセンタとの通信に関する動作を説明するフローチャートである。

【図4】カードの実施例の基本構成を示す機能ブロック図である。

【図5】カードの動作を説明するフローチャートである。

【図6】センタ装置の実施例の基本構成を示す機能ブロック図である。

【図7】センタ装置の動作のうち偽造カードの検出に関する動作を説明するフローチャートである。

【図8】センタ装置の動作のうちカード読取書込装置との間の通信に関する動作を説明するフローチャートである。

【図9】カード読取書込装置の認証手段およびカードの認証手段において用いられている認証方法を説明するシーケンスチャートである。

【図10】カードの認証手段の構成例を示す機能ブロック図である。

【図11】カード読取書込装置における認証手段の構成例を示す機能ブロック図である。

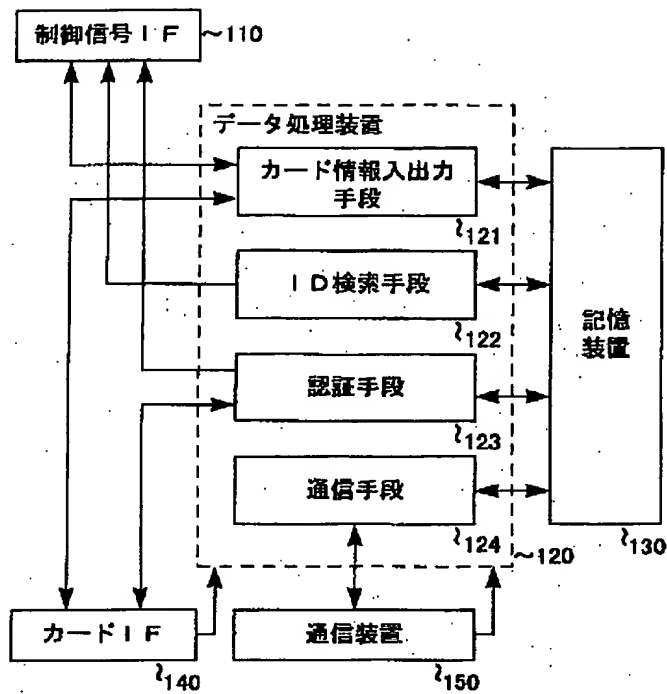
【図12】カード署名装置の実施例を示す機能ブロック図である。

【図13】本発明の偽造カード使用防止システムの一例を示す全体構成図である。

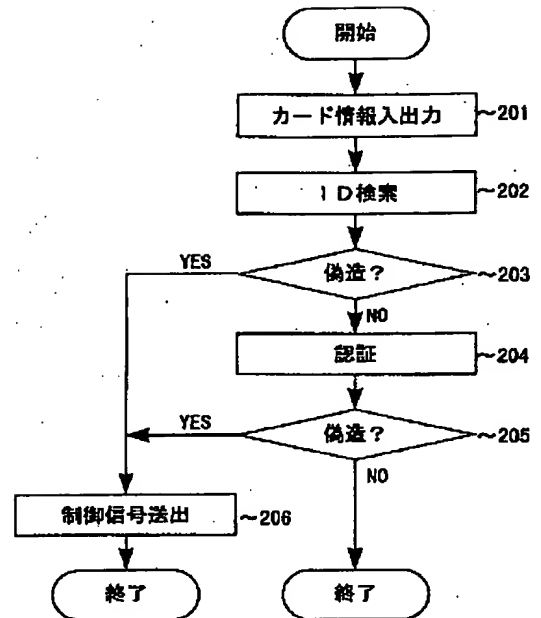
#### 【符号の説明】

- 1…カード読取書込装置
- 2…カード
- 3…センタ装置
- 4…外部装置
- 110…制御信号インタフェース
- 120, 420, 620…データ処理装置
- 130, 430, 630…記憶装置
- 140, 1202…カードインタフェース
- 150, 650…通信装置
- 410…インタフェース
- 1002…関数 $S_i$
- 1101…乱数発生器
- 1102, 1201…暗号関数
- 1103…セレクト
- 1104…比較器

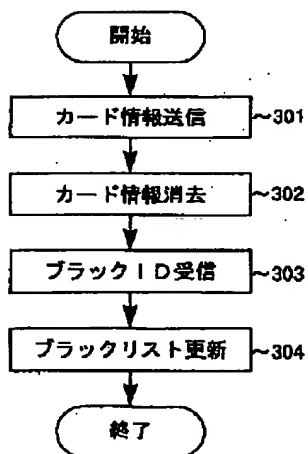
【図1】



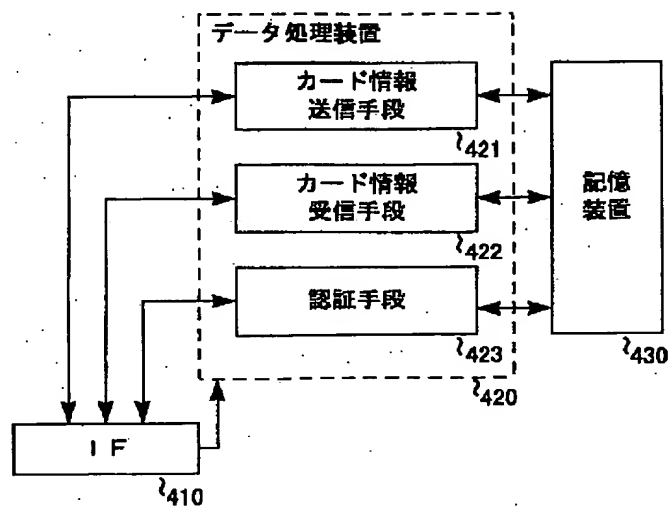
【図2】



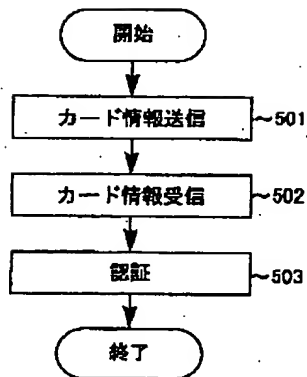
【図3】



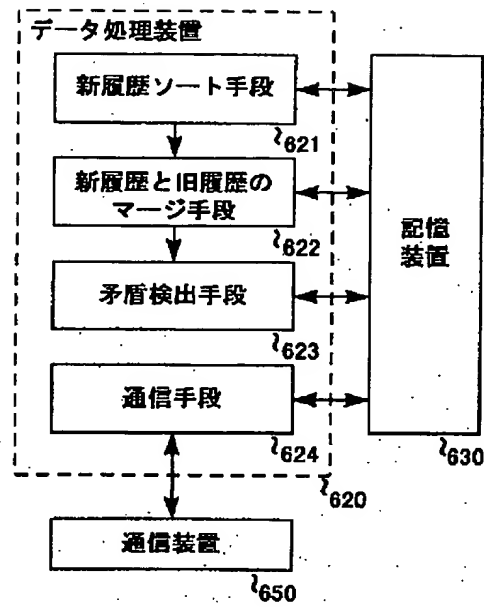
【図4】



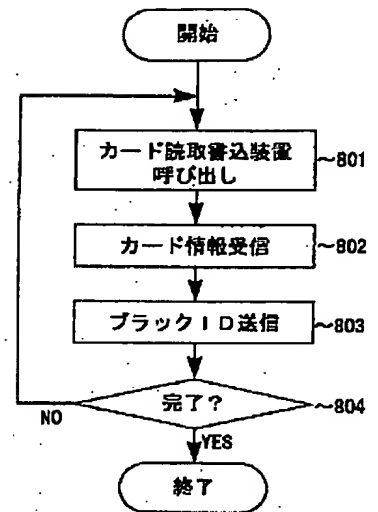
【図5】



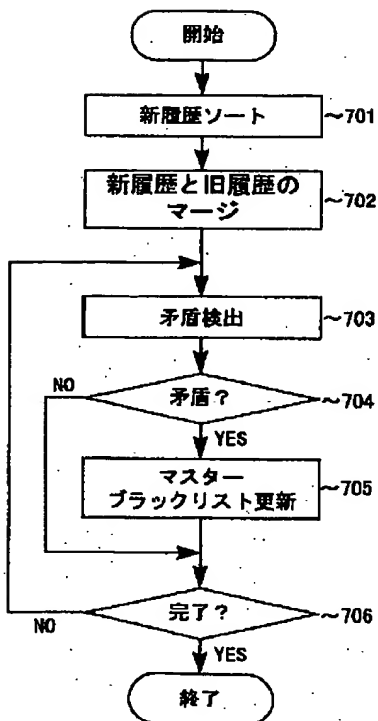
【図6】



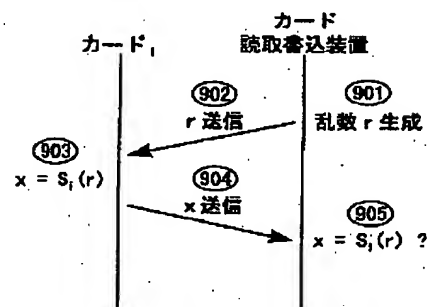
【図8】



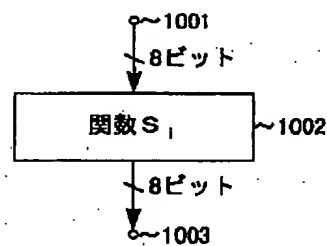
【図7】



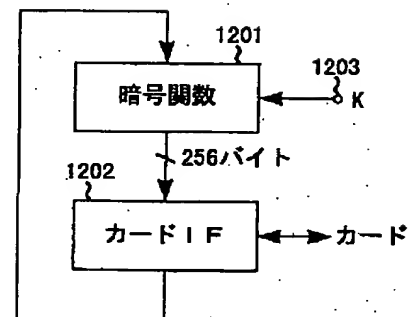
【図9】



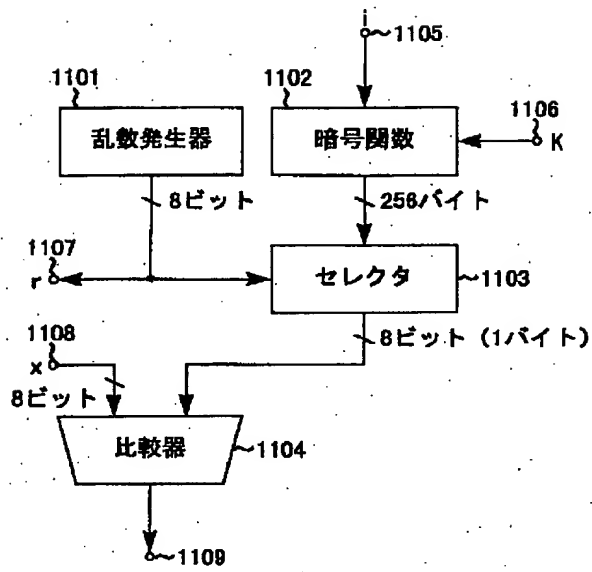
【図10】



【図12】



【図11】



【図13】

